IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF TWO ELECTRONIC DEVICES CURRENTLY IN THE CUSTODY OF THE BALTIMORE POLICE DEPARTMENT AT EVIDENCE CONTROL	**Case No.** 1:21-mj-2745 TMD
IN THE MATTER OF THE SEARCH OF A CERTAIN INSTAGRAM ACCOUNT STORED AT PREMISES CONTROLLED BY FACEBOOK, INC.	**Case No.** 1:21-mj-2746 TMD

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR TWO SEARCH WARRANTS

I, Shane Lettau, a Task Force Officer with the Federal Bureau of Investigation, being first duly sworn, hereby depose and state as follows:

PURPOSE OF THIS AFFIDAVIT

1. I submit this affidavit in support of applications for two search warrants. The first warrant seeks authorization to search of:

a. A Blue Apple iPhone recovered from Ronald JONES during his arrest and currently in custody of the Baltimore Police Department under unique property number 4761669 (**SUBJECT ELECTRONIC DEVICE 1**); and,

b. A white Apple iPhone recovered from Ronald JONES during his arrest and currently in custody of the Baltimore Police Department under unique property number 4761670 (**SUBJECT ELECTRONIC DEVICE 2**), (collectively, the **SUBJECT DEVICES**).

2. The **SUBJECT DEVICES** are further described in Attachment A-1 and are presently in the custody of the Baltimore Police Department Evidence Control Unit located at

601 E. Fayette Street, Baltimore, Maryland 20202 in the District of Maryland.

1. The second warrant would require Instagram, LLC ("Instagram"), a social-networking company owned by Facebook, Inc. and headquartered at 1601 Willow Road, Menlo Park, California (the **SERVICE PROVIDER**) to disclose to the government records and other information in its possession for the account "**bstreet_bo**" (the **SUBJECT ACCOUNT**) believed to belong and/or used by Ronald JONES and further described in Attachment A-2. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A), to require Instagram to disclose to the government records and other information in its possession, including the contents of communications, pertaining to the subscriber or customer associated with the **SUBJECT ACCOUNT.**

3. I submit that there is probable cause to believe that the **SUBJECT DEVICES** and **SUBJECT ACCOUNT** contain evidence of Possession of a Firearm by a Prohibited Person in violation of 18 U.S.C. § 922(g)(1), Possession with the Intent to Distribute a Controlled Dangerous Substance in violation of 21 U.S.C. § 841(a)(1)), and Possession of a Firearm in Furtherance of a Drug Trafficking Crime in violation of 18 U.S.C. § 924(c) (the **SUBJECT OFFENSES**). There is also probable cause to search the **SUBJECT DEVICES** and **SUBJECT ACCOUNT** as described Attachments A-1 and A-2 for evidence, instrumentalities, contraband, or fruits of these crimes as described in Attachments B-1 and B-2.

JURISDICTION

4. The Court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. See 18 U.S.C. § 2711(3)(A)(i).

AFFIANT BACKGROUND AND EXPERTISE

5. I am "an investigative or law enforcement officer" of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

6. I have been a duly sworn member of the BPD since January 29, 2002. I am currently assigned to the BPD's Criminal Investigation Division, working as a Task Force Officer for the FBI since May 2018. Since I began my career as a Baltimore Police Officer in January 2002, I have been assigned to the following units: Patrol Division, Mobile/Special Enforcement Teams, Organized Crime Division Narcotics Investigation, Violent Crime Impact Section Violent Repeat Offender Squad, Central Intelligence Division – HIDTA/ DEA and the Homicide Unit.

7. I am familiar with the language, terminology, and street slang used by persons who purchase and distribute CDS. I am also familiar with the prices and packaging and paraphernalia used to distribute and manufacture CDS. I have surveilled numerous narcotic transactions on the streets of Baltimore City and within the Baltimore Metropolitan Area. As a result of these observations, thousands of arrests have been made for CDS violations and narcotics transactions. Furthermore, I have conducted surveillance and enforcement activities in other states and in Africa as part of investigations of narcotics-related activity.

8. I have interviewed numerous confidential informants, cooperating witnesses, street level, mid-level, narcotics distributors/traffickers, and narcotics importers along with common narcotics users. This has provided me with an intimate insight into drug trafficking patterns. I am also familiar with the counter-surveillance techniques utilized against law

enforcement by drug traffickers.

9. I have testified over 20 times as an expert regarding the identification, packaging, and sale of CDS in the district, circuit, and federal courts of Baltimore, Maryland. I have also testified in state and federal grand juries on a number of occasions and as a result, the grand juries returned indictments against defendants.

10. As a result of these experiences and others, I am familiar with matters including, but not limited to, the means and methods used by drug-trafficking organizations to conceal, purchase, transport, store and distribute drugs, and to conceal profits or fruits generated from those transactions. Based on my knowledge, training and experience, I have become familiar with the methods of operations commonly used by individual drug-traffickers, including, but not limited to, the importation, manufacture, concealment and distribution of controlled substances. As a result of these experiences and others, I have become familiar with the techniques commonly used by drug-traffickers to facilitate and obfuscate illegal activity, including use of: telephones, mobile phones, prepaid phones, calling cards, public telephones, text-messaging, encrypted-messaging, counter-surveillance, false or fictitious identities and businesses, and coded communications to communicate with customers, suppliers, couriers, and other conspirators for the purpose of insulating themselves from the detection of law enforcement and rival drug-traffickers; that it is not unusual for drug-traffickers to establish such mobile / prepaid phones, vehicle registration and titling, applications for and payments of rental properties, including places of residence and storage facilities and utility services for these properties and the like, in the name of an associate, family member, fictitious or deceased person or business, wittingly or unwittingly; that drug-traffickers require the use of a telephone facility to negotiate times, places, schemes, and manners for importing, possessing, concealing, and distributing

controlled substances, and for arranging the concealment of proceeds derived from the sale of controlled substances; that drug-trafficking is an ongoing and evolving process that requires the development, use, and protection of a communication networks enabled by a market of publicly available and advertised encrypted messaging and calling services; that drug-traffickers regularly use coded language when speaking or writing to other drug-traffickers to confuse, disguise or otherwise thwart law enforcement's efforts to penetrate communication networks and telephone facilities engaged in drug-trafficking.

11. Through my training and prior experience, I know the following:

a. Firearms and drug trafficking are an ongoing and recurring criminal activity. As contrasted with crimes against persons, which tend to be discrete offenses, drug trafficking is an illegal commercial activity that is characterized by regular, repeated criminal activity.

b. Cellular telephones are an indispensable tool of the firearms and narcotics trafficking trade. Narcotic traffickers use cellular telephones, push-to-talk telephones, Short Message Service (SMS), electronic-mail, and similar electronic means and/or devices, often under fictitious names or names other than their own, in order to maintain contact with other conspirators and narcotic traffickers. In addition, narcotic traffickers will often change their cellphones following the arrest of a member of their Drug Trafficking Organization (DTO), or at random in order to frustrate law enforcement efforts.

c. Drug traffickers keep and maintain records of their various activities. Such records are regularly concealed in a suspect's automobile, residence, office, and on his person, and that they take various forms. Documents commonly concealed by traffickers, include but are not limited to notes in code, deposit slips, wired money transactions, hidden bank accounts, photographs of co-conspirators, various forms of commercial paper, personal address books, notebooks, records, receipts, ledgers, travel receipts (rental receipts, airline tickets, bus tickets, and/or train tickets) both commercial and private, money orders and other papers relating to the ordering, transportation, sale and distribution of controlled dangerous substances or other such documents which will contain identifying data on the co-conspirators. These items are kept in locations that are considered safe by the drug traffickers such as safety deposit boxes, residences, vehicles and on their person, where they have ready access to them. Drug traffickers often have several residences decreasing the likelihood of

detection by law enforcement;

d. Firearms and drug traffickers use cellular telephones and other electronic communications devices to facilitate illegal transactions. The electronically stored information on these devices is of evidentiary value in identifying other members of the firearms and drug trafficking conspiracy and establishing the relationship between these individuals, including photographs and other identifying information stored on these devices; they also use their cellphones to communicate on various social media platforms such as Facebook and Instagram; and,

e. Drug traffickers use computers or other electronic storage media, including smart phones, to store the records documents, take and store photographs and videos of co-conspirators, and contraband or items listed in paragraphs (c) and (d).

12. I also know, based on my training and experience, that individuals involved with drug trafficking and illegal firearm possession frequently use cellular telephones, communication devices, and other electronic media storage to further their illegal activities. Persons who have firearms tend to take photographs of the firearm and ammunition, which is stored on their electronic device. An individual may communicate with others in reference to the purchase of or the selling of firearms and CDS through their electronic devices. Individuals found with firearms and CDS often post pictures of evidence, fruits of the crime, and instrumentalities, on social media pages to show others with whom they are connected, and use cellular telephones to take these pictures.

13. I know also know from training and experience that felons in possession of handguns and those that are involved in drug trafficking often post evidence of their criminal activity on Instagram, e.g., pictures of firearms, CDS, currency, etc. Further, criminals will use Instagram itself as mode of communication to plan, conspire, and otherwise discuss criminal activities.

14. I know that Instagram often stores e-mail addresses, phone numbers, and other

manners of communication of its users. Identification of the phone numbers and email addresses used by the targets of this investigation can lead to further evidence of the **SUBJECT OFFENSES** through comprehensive analysis of phone contacts, subscribers, and cellular location.

15. Because I submitted preservation notices for the **SUBJECT ACCOUNT,** I believe that a search of this account will yield evidence of a crime since the account will contain evidence related to the **SUBJECT OFFENSES** and the events summarized below.

16. Because this affidavit is being submitted for the limited purpose of establishing probable cause to search the **SUBJECT DEVICES and SUBJECT ACCOUNT,** I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. I have not, however, excluded any information known to me that would defeat a determination of probable cause. The information contained in this affidavit is based upon my personal knowledge, my review of documents and intercepted conversations, as well as conversations with other law enforcement officers and other individuals. All conversations and statements described in this affidavit are related in substance and in part unless otherwise indicated.

PROBABLE CAUSE

17. On May 28, 2021, at approximately 6:00 P.M., detectives with the Baltimore City Police Department (BPD) Southwest District Action Team (DAT) conducted an investigation into drug trafficking activities in the vicinity of a Crown Gas Station in the 1800 block of Bloomingdale Road, Baltimore, Maryland. During the course of their investigation, a detective conducting covert surveillance recognized an individual known to the detectives based on prior encounters as Ronald JONES. JONES was wearing a grey hooded sweatshirt, and a

black hat, and carrying a grey Under Armour backpack. The detective observed JONES holding clear bottles that appeared to contain marijuana, and then showing the bottles to people as they approached the Crown to pump gas. JONES also readjusted an object in his front sweatshirt pocket on several occasions, and the detective was able to see what appeared to be the imprint of a firearm in his sweatshirt. Based on these observations, the detective believed that JONES was attempting to sell marijuana and was armed, and he alerted the arrest team.

18. Prior to the arrest team responding to the Crown, the detective conducting covert surveillance watched JONES walk away and enter the driver's seat of a burgundy 2013 Nissan Altima bearing West Virginia Temporary Tag 412598 that was parked nearby. A second individual entered the passenger side of the vehicle, and then JONES drove back to the Crown and parked at a pump. Both individuals remained in the vehicle with the doors open while conversing with others in the area.

19. The arrest team arrived at the Crown in a fully marked BPD patrol vehicle with departmentally issued tactical vests conspicuously marked "Police" on the front and rear. When detectives approached the Altima and exited the patrol vehicle, JONES and the other occupant fled the scene in the vehicle. Detectives followed the vehicle into the rear alley of the 3000 block of West North Avenue where the vehicle was abandoned, first by the unknown passenger and then, a short time later, by JONES on foot. Detectives pursued JONES on foot and apprehended him in the 2900 block of Westwood Street. As detectives pursued JONES, other law enforcement officers maintained surveillance of the abandoned Nissan Altima.

20. JONES was searched, at which time investigators recovered a clear bottle containing suspected marijuana, four Subxone strips, and the **SUBJECT DEVICES**

21. **SUBJECT ELECTRONIC DEVICE 1** was found in JONES' hooded sweatshirt

pocket immediately following his arrest. **SUBJECT ELECTRONIC DEVICE 2** was later found in JONES' front pants pocket when detectives searched him prior to being transported.

22. Detectives then searched the Nissan Altima and recovered the grey Under Armour backpack similar to that which was previously seen in the possession of JONES. Inside the backpack, the detectives found numerous bags and jars of marijuana, along with a digital scale.

23. Also inside the vehicle, they found an Amadeo Rossi, .44 caliber revolver handgun, Serial Number AB065394 loaded with one spent shell casing and four live .44 caliber rounds, along with additional marijuana.

24. The firearm was located beneath the driver's seat, towards the rear. The total amount of suspected marijuana was approximately 322 grams.

25. JONES is prohibited from possessing a firearm based on his prior criminal history, including a 2016 federal conviction for Possession of a Firearm and Ammunition by a Prohibited Person (JKB-16-0341) for which he received a sentence of 30 months' incarceration. As a result, he knew or should have known he was sentenced to more than one year of incarceration and therefore prohibited from possessing a firearm.

26. The **SUBJECT ACCOUNT** is identified as "bstreet_bo" and is believed to be utilized by Ronald JONES (AKA: "Bo") based on posted photographs and recognition of him through this and other investigations. Your affiant is aware that the account was previously subject to a federal search and seizure warrant signed by the Honorable Charles B. Day, Magistrate Judge of the United States District Court for the District of Maryland (20-MJ-1291-CBD) dated May 18, 2020. At the time, Jones was incarcerated following a violation of his federal probation; however, he has since been released and appears to have continued to use the **SUBJECT ACCOUNT**.

27. Examination of the previous search warrant returns revealed that JONES had photographs of various types of firearms that were sent to him from people including, but not limited to, photographs of handguns and assault rifles. These messages were not publicly posted and are therefore believed to have been transmitted through the private messaging service of Instagram known as "Direct Messages" (or "DMs.") Some of the identified firearm pictures had serial numbers, while the serial numbers for other firearms were not visible. And, on at least one occasion, Jones reached out to one of the prospective underground sellers to find out how much money the seller wanted for a posted gun. Based on these communications, investigators believe that Jones purchased an assault rifle from one of the individuals for $600.00 in April 2019.

28. Given these previous communications and that JONES has continued to use the **SUBJECT ACCOUNT**, it is foreseeable that evidence of how JONES purchased, possessed and/or used the firearm recovered during his May 28, 2021 arrest will be found in the **SUBJECT ACCOUNT** along with other evidence related to the **SUBJECT OFFENSES.**

BACKGROUND CONCERNING ELECTRONIC COMMUNICATIONS DEVICES

29. The fruits and instrumentalities of criminal activity are often concealed in digital form. Furthermore, digital camera technology is often used to capture images of tools and instrumentalities of pending criminal activity. The **SUBJECT DEVICES** have both digital storage capacity and digital camera capabilities.

30. Individuals engaged in firearms and drug trafficking offenses often use cell phones to communicate with suppliers, to place orders with suppliers, to communicate with customers, to receive orders from customers, and to arrange meeting times and locations for the distribution of controlled substances. The individuals engaging in firearms and drug trafficking will often use a combination of voice calls and text messages to coordinate drug transactions.

Individuals engaged in drug trafficking offenses also use digital storage devices to maintain telephone number "contact lists" of individuals who may have assisted in the planning of this and other criminal activity.

31. Firearms and narcotic traffickers often place nominal control and ownership of telephones in names other that their own to avoid detection of those telephones by government agencies. Even though telephones are in the names of other people, drug traffickers retain actual ownership, control, and use of the telephone, exercising dominion and control over them.

32. Criminals utilize different types of communication devices, and change the numbers to these communication devices frequently. This is done to avoid detection by law enforcement personnel. Also, as noted above, firearms and drug traffickers dedicate different communication devices for different aspects of the trafficking organization.

33. Cellular phones associated with firearms and drug traffickers include various types of evidence. Phones may contain relevant text messages or other electronic communications; they may contain electronic address books listing the phone numbers and other contact information associated with co-conspirators; and they may contain other types of information.

34. Criminals often take photos of themselves with firearms, large quantities of controlled substances, money, or high-end consumer items, like cars or watches. These "trophy" photos are often maintained on cellular telephones to be shared on social media, or as symbols of their success.

35. Finally, the mere fact of a cellular phone's call number, electronic serial number or other identifying information may be of evidentiary value as it may confirm that a particular cell phone is the phone identified during a wiretap, pen register, or other electronic investigation.

FORENSIC ANALYSIS OF ELECTRONIC COMMUNICATIONS DEVICES

36. Based on my training and experience, I know that electronic devices such as cellular phones (smartphones) can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. There is probable cause to believe that things that were once stored on the **SUBJECT DEVICES** may still be stored on those devices, for various reasons, as discussed in the following paragraphs.

37. As further described in Attachment B-1, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **SUBJECT DEVICES** were used, the purpose of its use, who used it, and when.

38. There is probable cause to believe that this forensic electronic evidence might be on the **SUBJECT DEVICES** because data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

39. Forensic evidence on a device can also indicate who has used or controlled the

device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

40. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

41. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

42. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

43. During this case and in numerous others involving complex DTOs, investigators have learned that the drug-trafficking organization relies heavily on electronic devices to facilitate drug trafficking. It is necessary to conduct a physical inspection of the electronic devices in order to obtain electronic communications and other information that might be stored on the seized phone and to determine whether any of the seized phone were the subject of wiretap, pen register or other investigation detailed herein. The phone may also contain data and communications that were not electronically intercepted due to encryption or for other reasons.

44. The device will be examined by persons qualified to perform the search /

examination, with any and all necessary and proper assistance, any and all electronic computing or data processing devices and associated peripheral equipment such as computer units, keyboards, central processing units, external or internal drives and/or other receiving devices and peripheral equipment such as printers, modems, associated telephone sets, and any other controlling devices and generate copies and photograph any evidence seized and any evidence therein. If needed, the processing may be conducted by a law enforcement entity or facility outside the state of Maryland.

45. Again, the **SUBJECT DEVICES** remain in the custody of law enforcement. The only known specifics of each phone requested for authorization to search are detailed in Attachment A-1 and the types of information expected to be recovered from the devices are listed in Attachment B-1.

BACKGROUND CONCERNING INSTAGRAM

46. From my review of publicly available information provided by Instagram about its service, including Instagram's "Privacy Policy," I am aware of the following about Instagram and about the information collected and retained by Instagram.

47. Instagram owns and operates a free-access social-networking website of the same name that can be accessed at http://www.instagram.com. Instagram allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and other information. Users can access Instagram through the Instagram website or by using a special electronic application ("app") created by the company that allows users to access the service through a mobile device.

48. Instagram permits users to post photos to their profiles on Instagram and otherwise share photos with others on Instagram, as well as certain other social-media services,

including Flickr, Facebook, and Twitter. When posting or sharing a photo on Instagram, a user can add to the photo: a caption; various "tags" that can be used to search for the photo (e.g., a user made add the tag #vw so that people interested in Volkswagen vehicles can search for and find the photo); location information; and other information. A user can also apply a variety of "filters" or other visual effects that modify the look of the posted photos. In addition, Instagram allows users to make comments on posted photos, including photos that the user posts or photos posted by other users of Instagram. Users can also "like" photos.

49. Instagram users may send photos and videos to select individuals or groups via Instagram Direct. Information sent via Instagram Direct does not appear in a user's feed, search history, or profile.

50. Instagram users also may communicate with other users, by Direct Messages or otherwise. Instagram collects and maintains copies of communications between users.

51. As explained herein, information stored in connection with an Instagram account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, an Instagram user's account activity, IP log, stored electronic communications, and other data retained by Instagram, can indicate who has used or controlled the Instagram account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the Instagram account at a relevant time. Further, Instagram account activity can show how and when the account was

accessed or used. For example, as described herein, Instagram logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Instagram access, use, and events relating to the crime under investigation. Additionally, Instagram builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Instagram "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Instagram account owner. Last, Instagram account activity may provide relevant insight into the Instagram account owner's state of mind as it relates to the offense under investigation. For example, information on the Instagram account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

52. Based on the information above, the computers of Instagram are likely to contain all the material described above with respect to the **SUBJECT ACCOUNT**, including stored electronic communications and information concerning subscribers and their use of Instagram, such as account access information, which would include information such as the IP addresses and devices used to access the account, as well as other account information that might be used to identify the actual user or users of the account at particular times.

53. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant

to require Instagram/Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B-2. Upon receipt of the information described in Section I of Attachment B-2, government-authorized persons will review that information to locate the items described in Section II of Attachment B-2.

CONCLUSION

54. Accordingly, there is probable cause to believe that evidence of the **SUBJECT OFFENSES** will be found from an analysis of the recovered **SUBJECT DEVICES** and the **SUBJECT ACCOUNT** described in Attachments A-1 and A-2.

55. WHEREFORE, in consideration of the facts presented, I respectfully request that the Court issue the proposed search warrants for the **SUBJECT DEVICES and SUBJECT ACCOUNT**, and authorize the search and seizure of the items described in Attachments A-1 and A-2, for the purposes of identifying the electronically stored data particularly described in Attachments B-1 and B-2.

REQUEST FOR NIGHT-TIME AUTHORIZATION

56. There is good cause for the Court to authorize the requested searches at any time of the day or night. The **SUBJECT DEVICES** are already in law enforcement custody, and it is reasonable to allow law enforcement to execute the requested searches at any hour of the day, even during the evening or night, if doing so is convenient for the investigators or examiners. Because the devices are already in law enforcement custody, there will be no prejudice to any other person from this request.

57. Likewise, pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of the Instagram search warrant. The

government will execute this warrant by serving it on Instagram. Because the warrant will be served on Instagram, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Respectfully submitted,

Shane Lettau
Task Force Officer
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 5 day of October, 2021

The Honorable Thomas M. DiGirolamo
United States Magistrate Judge

ATTACHMENT A-1
Device to be Searched

The following devices, currently in the custody of the BPD in the District of Maryland:

a. A Blue Apple iPhone recovered from Ronald JONES during his arrest and currently in custody of the Baltimore Police Department under unique property number 4761669 (**SUBJECT ELECTRONIC DEVICE 1**); and,

b. A white Apple iPhone recovered from Ronald JONES during his arrest and currently in custody of the Baltimore Police Department under unique property number 4761670 (**SUBJECT ELECTRONIC DEVICE 2**).

ATTACHMENT A-2
Property to be Searched

This warrant applies to information associated with the following Instagram account from May 18, 2020 to present:

"bstreet_bo"

that is stored at premises owned, maintained, controlled, or operated by Facebook, Inc, a company that is owned by Facebook, Inc. and headquartered in Menlo Park, California.

ATTACHMENT B-1
Items to be Seized

All records contained in the items described in Attachment A-1, which constitute evidence of the **SUBJECT OFFENSE,** including but not limited to those outlined below:

1. Contact logs that refer or relate to the user of any and all numbers on the Subject Electronic Devices.

2. Call logs reflecting date and time of received calls.

3. Any and all digital images and videos of persons associated with this investigation.

4. Text messages to and from the **SUBJECT DEVICES** that refer or relate to the crimes under investigation.

5. Records of incoming and outgoing voice communications that refer or relate to the crimes under investigation.

6. Voicemails that refer or relate to the crimes under investigation.

7. Voice recordings that refer or relate to the crimes under investigation.

8. Any data reflecting the phone's location.

9. Contact lists.

10. Any and all records related to the location of the user(s) of the devices.

11. For the **SUBJECT DEVICES**:
    a. Evidence of who used, owned, or controlled the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;
    d. evidence of the attachment to the **SUBJECT DEVICES** of other storage devices or similar containers for electronic evidence;
    e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the Devices;
    f. evidence of the times the **SUBJECT DEVICES** were used;

g. passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT DEVICES** ;
h. documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the **SUBJECT DEVICES**; and,
i. contextual information necessary to understand the evidence described in this attachment.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

1. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

2. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

3. "scanning" storage areas to discover and possible recover recently deleted files;

4. "scanning" storage areas for deliberately hidden files; or

5. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps

to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated, absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

Attachment B-2
Particular Things to be Seized

I. Information to be disclosed by Instagram (Facebook) from May 18, 2020 to Present

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of Instagram, including any messages, records, files, logs, or information that have been deleted but are still available to Instagram, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Instagram is required to disclose the following information to the government for the account listed in Attachment A-2:

(a) All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, phone numbers, gender, hometown, occupation, and other personal identifiers;

(b) All past and current usernames associated with the account;

(c) The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up

(d) All activity logs including IP logs and other documents showing the IP address, date, and time of each login to the account, as well as any other log file information;

(e) All information regarding the particular device or devices used to login to or access the account, including all device identifier information or cookie information, including all information about the particular device or devices used to access the account and the date and time of those accesses;

(f) All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes

(g) A list of all of the people that the user follows on Instagram and all people who are following the user (i.e., the user's "following" list and "followers" list), as well as any friends of the user;

(h) A list of all users that the account has "unfollowed" or blocked;

(i) All privacy and account settings;

(j) All information about connections between the account and third-party websites and applications; and

(k) All records pertaining to communications between **SERVICE PROVIDER** and any person regarding the user or the user's Instagram account, including contacts with support services, and all records of actions taken, including suspensions of the account.

(l) For the time period **May 18, 2020 to Present**:

i. All communications or other messages sent or received by the account:

ii. All user content created, uploaded, or shared by the account, including any comments made by the account on photographs or other content;

iii. All photographs and images in the user gallery for the account;

iv. All location data associated with the account, including geotags; and

v. All data and information that has been deleted by the user.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of the **SUBJECT OFFENSES** since May 18, 2020 to present, including, for the account identified on Attachment A-2, information pertaining to the following matters:

(a) All images, messages, communications, calendar entries, and contacts related to the **SUBJECT OFFENSES**;

(b) Evidence indicating how and when the Instagram account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Instagram account owner;

(c) Evidence indicating the Instagram account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the user ID about matters relating to offenses under investigation.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, document, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent

reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.